DUMPSARENA

Certified Wireless Security Professional (CWSP)

CWNP CWSP-208

Version Demo

Total Demo Questions: 13

Total Premium Questions: 131

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, WLAN Discovery Techniques	5
Topic 2, WLAN Intrusion and Attack Techniques	15
Topic 3, 802.11 Protocol Analysis	26
Topic 4, Wireless Intrusion Prevention Systems	16
Topic 5, WLAN Security Design, Implementation, and Management	69
Total	131

QUESTION NO: 1

As a part of a large organization's security policy, how should a wireless security professional address the problem of rogue access points?

A. Use a WPA2-Enterprise compliant security solution with strong mutual authentication and encryption for network access of corporate devices.

B. Hide the SSID of all legitimate APs on the network so that intruders cannot copy this parameter on rogue APs.

C. Conduct thorough manual facility scans with spectrum analyzers to detect rogue AP RF signatures.

D. A trained employee should install and configure a WIPS for rogue detection and response measures.

E. Enable port security on Ethernet switch ports with a maximum of only 3 MAC addresses on each port.

ANSWER: D

Explanation:

A trained employee should install and configure a WIPS for rogue detection and response measures. A wireless intrusion prevention system provides the scalable, continuous wireless monitoring that a large organization needs to identify unauthorized access points and distinguish them from neighboring devices that are outside the organization's control. Proper WIPS deployment uses distributed sensors or compatible access points to collect RF and 802.11 management-frame information, correlate observed devices with the authorized WLAN inventory and wired-network data, and alert security personnel when a true rogue is identified. This supports a defined incident-response process: investigate the device, locate it, remove its wired connection or otherwise contain the threat using authorized procedures, and document the event. Continuous monitoring is important because rogue devices can be connected temporarily and may not be present during an occasional assessment. A trained administrator is also essential because classification and response actions must be carefully configured to avoid disrupting legitimate systems or devices outside the organization's authority. CWNP's CWSP program specifically covers wireless threat detection, monitoring, and security controls: CWNP CWSP certification. NIST also recommends continuous monitoring and documented security controls for WLAN environments: NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks.

QUESTION NO: 2

Given: Many corporations configure guest VLANs on their WLAN controllers that allow visitors to have Internet access only. The guest traffic is tunneled to the DMZ to prevent some security risks.

In this deployment, what risks are still associated with implementing the guest VLAN without any advanced traffic monitoring or filtering features enabled? (Choose 2)

A. Intruders can send spam to the Internet through the guest VLAN.

B. Peer-to-peer attacks can still be conducted between guest users unless application-layer monitoring and filtering are implemented.

C. Unauthorized users can perform Internet-based network attacks through the WLAN.

D. Guest users can reconfigure AP radios servicing the guest VLAN unless unsecure network management protocols (e.g. Telnet, HTTP) are blocked.

E. Once guest users are associated to the WLAN, they can capture 802.11 frames from the corporate VLANs.

ANSWER: A C

Explanation:

Intruders can send spam to the Internet through the guest VLAN because an Internet-only guest network still provides a route to external mail systems, web forms, and other Internet services. Tunneling guest traffic to a DMZ and isolating it from internal corporate resources limits exposure to the enterprise network, but it does not inherently inspect, rate-limit, reputation-filter, or block abusive outbound activity. A malicious or compromised guest device can therefore use the organization's Internet connection as an egress path for unsolicited messages or similar abuse.

Unauthorized users can perform Internet-based network attacks through the WLAN for the same reason: basic guest VLAN segmentation controls where traffic may go, not whether the permitted Internet traffic is malicious. Without advanced monitoring or filtering, guests may conduct reconnaissance, exploit attempts, password attacks, denial-of-service activity, or other attacks against external systems. Effective guest-network security should combine segmentation with controls such as firewall policy enforcement, intrusion prevention, DNS and web filtering, logging, anomaly detection, and egress rate limits. NIST's wireless-network guidance discusses the importance of applying security controls to wireless traffic and network boundaries; see NIST SP 800-153. Additional practical network-segmentation guidance is available from CISA.

QUESTION NO: 3

You are implementing an 802.11ac WLAN and a WIPS at the same time. You must choose between integrated and overlay WIPS solutions. Which of the following statements is true regarding integrated WIPS solutions?

A. Integrated WIPS always perform better from a client throughput perspective because the same radio that performs the threat scanning also services the clients.

B. Integrated WIPS use special sensors installed alongside the APs to scan for threats.

C. Many integrated WIPS solutions that detect Voice over Wi-Fi traffic will cease scanning altogether to accommodate the latency sensitive client traffic.

D. Integrated WIPS is always more expensive than overlay WIPS.

ANSWER: C

Explanation:

Many integrated WIPS solutions that detect Voice over Wi-Fi traffic will cease scanning altogether to accommodate the latency sensitive client traffic. Integrated WIPS commonly reuses access-point radios for both client service and wireless threat detection. Because a radio cannot continuously serve associated clients while also performing off-channel scanning, the platform must schedule scanning around client-service demands. Voice traffic is especially sensitive to delay, jitter, and packet loss; therefore, an integrated design may defer, reduce, or suspend scanning while voice calls are active to preserve call quality. The precise behavior is vendor- and configuration-dependent, but this tradeoff is a fundamental consideration when evaluating integrated WIPS: security visibility can be reduced during periods in which the serving radio must prioritize real-time client traffic. This is why requirements for uninterrupted, dedicated RF monitoring can favor an overlay architecture with separate sensors. CWNP describes CWSP as covering WLAN threat detection and wireless intrusion prevention concepts in its CWSP certification overview. Cisco also documents that access-point radio operations must account for real-time voice requirements in its wireless controller voice configuration guidance.

QUESTION NO: 4

What is one advantage of using EAP-TTLS instead of EAP-TLS as an authentication mechanism in an 802.11 WLAN?

A. EAP-TTLS sends encrypted supplicant credentials to the authentication server, but EAP-TLS uses unencrypted user credentials.

B. EAP-TTLS supports client certificates, but EAP-TLS does not.

C. EAP-TTLS does not require an authentication server, but EAP-TLS does.

D. EAP-TTLS does not require the use of a certificate for each STA as authentication credentials, but EAP-TLS does.

ANSWER: D

Explanation:

EAP-TTLS does not require the use of a certificate for each STA as authentication credentials, but EAP-TLS does. This is a significant deployment advantage when an organization does not have the infrastructure or operational processes needed to issue, distribute, renew, revoke, and securely store an individual client certificate on every wireless station. Both methods use a TLS-protected exchange and require the authentication server to present a certificate so that the client can validate the

server and establish a protected channel. With EAP-TLS, however, mutual certificate-based authentication is fundamental: the authentication server also validates a client certificate presented by the STA. EAP-TTLS instead establishes the outer TLS tunnel using the server certificate, then carries an inner authentication method through that encrypted tunnel. The inner method can use credentials such as a username and password, avoiding the mandatory per-STA client-certificate requirement of EAP-TLS. This can simplify onboarding and credential lifecycle management while retaining confidentiality for the inner authentication exchange. In practice, administrators must still correctly validate the server certificate on clients, because that validation protects users against rogue authentication servers. See the EAP-TLS specification (RFC 5216) and the EAP-TTLS specification (RFC 5281).

QUESTION NO: 5

Given: AAA is an architectural framework used to provide three separate security components in a network. Listed below are three phrases that each describe one aspect of the AAA framework.

Option-1 — This AAA function is performed first and validates user identify prior to determining the network resources to which they will be granted access.

Option-2 — This function is used for monitoring and auditing purposes and includes the collection of data that identifies what a user has done while connected.

Option-3 — This function is used to designate permissions to a particular user.

What answer correctly pairs the AAA component with the descriptions provided above?

A. Option-1 – Access ControlOption-2 – AuthorizationOption-3 – Accounting

B. Option-1 – AuthenticationOption-2 – AccountingOption-3 – Association

C. Option-1 – AuthorizationOption-2 – Access ControlOption-3 – Association

D. Option-1 – AuthenticationOption-2 – AccountingOption-3 – Authorization

ANSWER: D

Explanation:

Option-1 – Authentication; Option-2 – Accounting; Option-3 – Authorization correctly maps each described function to the AAA security framework. Authentication is the initial process of establishing or verifying the identity of a user, device, or service before access decisions are made. In a wireless enterprise environment, this commonly occurs through credentials and an authentication method such as IEEE 802.1X/EAP, often with a RADIUS server participating in the decision.

Accounting is the collection of session and usage information for monitoring, auditing, reporting, and potentially billing. Typical accounting records can identify when a session began and ended, the user or device identity, and traffic or connection-related details. These records help an organization maintain visibility into network use and investigate security events.

Authorization follows successful authentication and determines what an identified user is permitted to access or do. Authorization is policy-driven and can assign permissions, roles, VLANs, access-control lists, or other restrictions appropriate to that authenticated identity. This sequence—verify identity, apply permissions, and record activity—is the core operational model of AAA. See the IETF AAA Architecture RFC 3539 and Cisco's AAA security overview.

QUESTION NO: 6

Given: A WIPS detects an unknown access point broadcasting an SSID similar to a corporate SSID. The security team must determine whether it is a true rogue AP connected to the corporate wired network or a neighboring device outside the organization.

What information is most useful for making this determination? (Choose 2)

A. An up-to-date inventory of authorized AP MAC addresses and locations.

B. Wired-network correlation showing that the device is connected to the corporate network.

C. The strongest RSSI reading observed by a wireless sensor.

D. The SSID advertised in the device's beacon frames.

E. The number of nearby client probe requests.

ANSWER: A B

Explanation:

An accurate inventory of authorized access points lets the WIPS exclude known corporate infrastructure from rogue classification. Wired-side correlation is also essential because a true rogue AP is normally identified by evidence that its MAC address, clients, or traffic can be correlated to the organization's wired network. This distinguishes an internal threat from a neighboring AP that merely appears in the RF environment.

Signal strength can assist with physically locating a device, but it does not prove that the device is connected to the corporate network. The SSID alone is also insufficient because attackers and neighboring networks can use any SSID.

QUESTION NO: 7

During WLAN infrastructure staging, an organization wants to reduce exposure of access-point and controller management interfaces before devices are placed into production.

Which two actions are appropriate hardening controls? (Choose 2)

A. Restrict management access to a dedicated management network and authorized administrator addresses.

B. Disable cleartext and unused management services such as Telnet and HTTP.

C. Retain default administrative credentials until the first scheduled maintenance window.

D. Publish controller management addresses so users can report connectivity problems.

E. Permit guest VLAN clients to reach management interfaces for troubleshooting.

ANSWER: A B

Explanation:

Restricting management access to a dedicated management network and authorized administrator addresses limits the systems that can initiate management sessions. This reduces exposure to untrusted user and guest networks.

Disabling cleartext and unused management services, such as Telnet and HTTP where secure alternatives are available, prevents administrators from inadvertently using insecure protocols and reduces the management attack surface.

Using default credentials is a significant management-interface risk, not a hardening measure. Publishing management addresses and allowing management access from guest networks create unnecessary exposure.

QUESTION NO: 8

In a WPA2-Personal WLAN, what statements correctly describe the Group Temporal Key (GTK)? (Choose 2)

A. It is shared by the AP and associated clients for group-addressed traffic.

B. It is delivered to the client encrypted during Message 3 of the 4-Way Handshake.

C. It is unique to each client and protects that client's unicast frames.

D. It is the WPA2-Personal passphrase transmitted by the AP after association.

E. It is derived only from the client MAC address and the AP BSSID.

ANSWER: A B

Explanation:

The GTK is shared by the access point and the associated clients in a BSS and is used to protect group-addressed traffic such as broadcast and multicast frames. During the 4-Way Handshake, the authenticator distributes the GTK to a client in Message 3, encrypted with the key-encryption key derived from that client's PTK.

Unlike a PTK, the GTK is not unique to one client association. The passphrase itself is used to derive the PMK; it is not transmitted as the GTK. The GTK also does not provide confidentiality for individually addressed unicast traffic, which uses the pairwise temporal key.

QUESTION NO: 9

Given: ABC Hospital wishes to create a strong security policy as a first step in securing their 802.11 WLAN.

Before creating the WLAN security policy, what should you ensure you possess?

A. Awareness of the exact vendor devices being installed

B. Management support for the process

C. End-user training manuals for the policies to be created

D. Security policy generation software

ANSWER: B

Explanation:

Management support for the process is essential before developing a WLAN security policy because policy is an organizational governance document, not merely a technical configuration guide. Senior management sponsorship establishes the authority to define security requirements, assign ownership, approve funding, and require compliance across departments. For a hospital, this support is especially important because WLAN protections may affect clinical workflows, mobile devices, visitor access, protected health information, and regulatory obligations. Management backing also enables the organization to perform risk assessment, resolve competing operational priorities, and apply enforcement consistently when exceptions or violations arise. A policy developed without this authority may be technically sound but lack the resources, organizational acceptance, and enforcement mechanism needed to be effective. NIST explains that organization-wide information-security policy is established at the senior-management level and provides the foundation for subsequent policies, standards, and procedures. CWNP security practice likewise treats policy definition and organizational commitment as foundational to a defensible wireless-security program. See NIST SP 800-12 Rev. 1 and the CWNP CWSP certification overview.

QUESTION NO: 10

You work as the security administrator for your organization. In relation to the WLAN, you are viewing a dashboard that shows security threat, policy compliance and rogue threat charts. What type of system is in view?

A. Wireshark Protocol Analyzer

B. Wireless VPN Management Systems

C. Wireless Intrusion Prevention System

D. Distributed RF Spectrum Analyzer

E. WLAN Emulation System

ANSWER: C

Explanation:

Wireless Intrusion Prevention System is correct because a WIPS is purpose-built to continuously monitor the wireless environment, identify security-relevant wireless activity, classify potential threats, and present the results through centralized dashboards, alerts, reports, and policy-compliance views. Its sensors or integrated access points observe management, control, and data traffic over the air, allowing the system to detect unauthorized access points and clients, evil-twin behavior, ad hoc networks, denial-of-service conditions, and other wireless attacks. A WIPS dashboard commonly correlates these observations into security-threat and rogue-threat classifications so an administrator can assess risk and prioritize response actions.

Policy-compliance reporting is also a core WIPS function. The system can compare observed WLAN behavior against organizational requirements, such as approved SSIDs, authentication and encryption settings, authorized infrastructure, and permitted device configurations. This combination of threat detection, rogue identification, and compliance monitoring distinguishes a WIPS operational view from a tool focused only on packet inspection or RF energy analysis. CWNP describes CWSP as covering wireless intrusion prevention systems and WLAN security monitoring; see CWNP CWSP Certification. Cisco's wireless intrusion prevention documentation also describes rogue detection and wireless threat monitoring capabilities: Cisco Wireless Intrusion Prevention System overview.

QUESTION NO: 11

What properties of WEP make active and passive cryptographic attacks practical? (Choose 2)

A. Its 24-bit IV space causes IV values to repeat.

B. Its CRC-32 integrity check is linear and can be manipulated.

C. It derives a unique AES pairwise key for every transmitted frame.

D. It uses a cryptographic MIC that prevents deliberate frame modification.

E. It encrypts the SSID, preventing attackers from collecting relevant traffic.

ANSWER: A B

Explanation:

WEP uses a 24-bit initialization vector, which is too small to prevent IV reuse on a busy WLAN. Repeated IVs and weaknesses in RC4 key scheduling allow attackers who collect sufficient traffic to analyze related keystreams and recover key material. WEP also uses a linear CRC-32 integrity check value. CRC-32 is designed to detect accidental errors, not deliberate modification, so an attacker can alter ciphertext and adjust the ICV in predictable ways.

WEP does not use a unique pairwise AES key for each client, and it does not use a cryptographic MIC comparable to CCMP integrity protection. The SSID is not a secret cryptographic input that prevents WEP attacks.

QUESTION NO: 12

Corporate laptop computers are frequently used on public wireless hot-spots. The security policy must reduce the risk that another user on the same hot-spot can discover services on, or initiate unsolicited connections to, a corporate laptop.

Which two controls should the policy require? (Choose 2)

A. Require a restrictive host-based firewall profile for public networks.

B. Disable file sharing, printer sharing, and network discovery on public networks.

C. Require a VPN for all connectivity to corporate resources.

D. Require public hot-spots to use MAC-address filtering.

E. Require every public hot-spot to present a captive portal.

ANSWER: A B

Explanation:

A host-based personal firewall using a restrictive public-network profile is an effective control because it blocks unsolicited inbound connections even when the laptop is connected to an untrusted Layer 2 network. This protection remains effective regardless of the hotspot operator's configuration.

Disabling file sharing, printer sharing, and network discovery on public-network profiles further reduces the services that a nearby peer can identify or attack. These controls directly address local peer-to-peer exposure.

A VPN can protect traffic to corporate resources, but it does not necessarily prevent another hotspot user from attempting local connections to the laptop. MAC filtering and captive portals are controls administered by the hotspot operator and do not provide a dependable endpoint protection policy.

QUESTION NO: 13

Given: Your company has just completed installation of an IEEE 802.11 WLAN controller with 20 controller-based APs. The CSO has specified PEAPv0/EAP-MSCHAPv2 as the only authorized WLAN authentication mechanism. Since an LDAP-compliant user database was already in use, a RADIUS server was installed and is querying authentication requests to the LDAP server.

Where must the X.509 server certificate and private key be installed in this network?

A. Supplicant devices

B. LDAP server

C. Controller-based APs

D. WLAN controller

E. RADIUS server

ANSWER: E

Explanation:

RADIUS server is correct because it is the authentication server that terminates the outer Protected Extensible Authentication Protocol version zero tunnel. In PEAPv0/EAP-MSCHAPv2, the wireless client first establishes a TLS-protected channel directly with the RADIUS/EAP server. To authenticate that server and create the TLS session, the RADIUS server presents its X.509 server certificate and proves possession of the corresponding private key during the TLS handshake. The client validates the certificate according to its configured trust settings, including the issuing certification authority and, where configured, the expected server identity.

After the protected tunnel has been established, EAP-MSCHAPv2 authentication occurs within that encrypted channel. The RADIUS server can use the LDAP directory as its identity store or as a source of account information, but the LDAP service is not the TLS endpoint for PEAP in this design. The controller and its access points act as authenticators and relay EAP messages between the supplicant and the RADIUS server; they do not terminate the PEAP TLS tunnel. CWNP describes enterprise WLAN authentication as involving the supplicant, authenticator, and authentication server roles. See CWNP CWSP certification information and the TLS protocol requirements in RFC 5216.